Sub a1

## CLAIMS

1. A method for securely communicating packets between a first computer device and a second computer device through a packet-switched data transmission network comprising intermediate computer devices, where at least one of said computer devices performs a network address translation and/or a protocol conversion, the method comprising the steps of

- determining what network address translations, if any, occur on packets transmitted between the first computer device and the second computer device,
- taking packets conforming to a first protocol and encapsulating them into packets conforming to a second protocol, which second protocol is capable of traversing network address translations,
- transmitting said packets conforming to said second protocol from the first computer device to the second computer device and
- decapsulating said transmitted packets conforming to said second protocol into packets conforming to said first protocol.

2. A method according to claim 1, wherein the step of taking packets conforming to a first protocol and encapsulating them into packets conforming to a second protocol comprises the substeps of

- taking packets conforming to the Internet Protocol,
- processing said packets according to the IPSEC protocol suite and

- encapsulating the processed packets into packets conforming to the User Datagram Protocol.

3. A method according to claim 1, wherein the step of taking packets conforming to a first protocol and encapsulating them into packets conforming to a second protocol comprises the substeps of
- taking packets conforming to the Internet Protocol,
- processing said packets according to the IPSEC protocol suite and
- encapsulating the processed packets into packets conforming to the Transmission Control Protocol.

4. A method according to claim 1, further comprising the step of compensating for the network address translations on said second protocol in the packets that are transmitted from the first computer device to the second computer device.

5. A method according to claim 4, wherein said step of compensating for the network address translations comprises a step of performing address translation based on the information obtained in the step of determining what network address translations, if any, occur on packets transmitted between the first computer device and the second computer device.

6. A method according to claim 5, wherein said step of

compensating for the network address translations further comprises a step of performing port number translation based on the information obtained in the step of determining what network address translations, if any, occur on packets transmitted between the first computer device and the second computer device.

7. A method according to claim 1, additionally comprising the step of periodically transmitting keepalive packets between the first computer device and the second computer device to ensure that the network address translations, if any, occurring on packets transmitted between the first computer device and the second computer device stay the same.

8. A method for conditionally setting up a secure communication connection between a first computer device and a second computer device through a packet-switched data transmission network comprising intermediate computer devices, where at least one of said computer devices performs a network address translation and/or a protocol conversion, the method comprising the steps of

- finding out, whether or not the second computer device supports a communication method where: it is determined what network address translations, if any, occur on packets transmitted between the first computer device and the second computer device; packets

are taken that conform to a first protocol and encapsulated into packets that conform to a second protocol, which second protocol is capable of traversing network address translations; said packets conforming to said second protocol are transmitted from the first computer device to the second computer device; and said transmitted packets conforming to said second protocol are decapsulated into packets conforming to said first protocol,

- as a response to a finding indicating that the second computer device supports said communication method, setting up a secure communication connection between the first computer device and the second computer device in which communication connection said communication method is employed and

- as a response to a finding indicating that the second computer device does not support said communication method, disabling the use of said communication method between the first and the second computer devices.

9. A method for tunnelling packets between a first computer device and a second computer device through a packet-switched data transmission network comprising intermediate computer devices, where at least one of said computer devices performs a network address translation and/or a protocol conversion, the method comprising the steps of

- establishing a bidirectional tunnelling mode between the first

computer device and the second computer device by exchanging packets conforming to a secure communication protocol,

- taking packets conforming to a first protocol and encapsulating them at the first computer device into packets conforming to a second protocol, which second protocol is capable of traversing network address translations,

- transmitting said packets conforming to said second protocol from the first computer device to the second computer device,

- decapsulating said transmitted packets conforming to said second protocol into packets conforming to said first protocol at the second computer device,

- obtaining information about the address translations occurred on packets transmitted between the first computer device and the second computer device and

- using said obtained information to modify the established bidirectional tunnelling mode between the first computer device and the second computer device.

10. A method according to claim 9, wherein the step of obtaining information about the address translations occurred on packets transmitted between the first computer device and the second computer device comprises the substeps of

- transmitting a packet between the first computer device and the second computer device, said packet comprising a header part and a

payload part, and

- comparing a network address transmitted in said payload part to a network address transmitted in said header part in order to find out what changes have occurred on said network address transmitted in said header part.

11. A method according to claim 9, additionally comprising the step of periodically transmitting keepalive packets between the first computer device and the second computer device to ensure that the network address translations, if any, occurring on packets transmitted between the first computer device and the second computer device stay the same.

12. A method according to claim 9, wherein the step of using said obtained information to modify the operation of the tunnelling of packets comprises the substep of introducing an address translation before the encapsulation of packets in order to compensate for the network address translations that occur on packets transmitted between the first computer device and the second computer device.

13. A method according to claim 9, wherein the step of using said obtained information to modify the operation of the tunnelling of packets comprises the substep of introducing an address

translation after the decapsulation of packets in order to compensate for the network address translations that occur on packets transmitted between the first computer device and the second computer device.

14. A method for tunnelling packets between a first computer device and a second computer device through a packet-switched data transmission network comprising intermediate computer devices, in which data transmission network there exists a security protocol comprising a key management connection that employs a specific packet format for key management packets, the method comprising the steps of

- encapsulating data packets that are not key management packets into said specific packet format for key management packets,
- transmitting said data packets encapsulated into the specific packet format from the first computer device to the second computer device,
- discriminating at the second computer device the data packets encapsulated into the specific packet format from actual key management packets and
- decapsulating the data packets encapsulated into the specific packet format.

15. A method according to claim 14, wherein the step of

encapsulating data packets that are not key management packets comprises the substeps of

- encapsulating data packets that are not key management packets into a key management packet format specified by the Internet Key Exchange protocol which defines a certain Initiator Cookie field and

- inserting into the Initiator Cookie field of an encapsulated data packet a value indicating that the encapsulated packet is a data packet and not a key management packet.

16. A method for securely communicating packets between a first computer device and a second computer device through a packet-switched data transmission network comprising intermediate computer devices, where at least one of said computer devices performs a network address translation and/or a protocol conversion and where a security protocol exists comprising a key management connection, the method comprising the steps of

- for determining what network address translations, if any, occur on packets transmitted between the first computer device and the second computer device: establishing a key management connection according to said security protocol between the first computer device and the second computer device; composing an indicator packet with a header part and a payload part of which both

comprise the network addresses of the first computer device and the second computer device as seen by the node composing said packet; transmitting and receiving said indicator packet within the key management connection; and comparing in the received indicator packet the addresses contained in the header part and the payload part, and

- using the information concerning the determined occurrences of network address translations to securely communicating packets between the first computer device and the second computer device.

17. A method according to claim 16, wherein the security protocol determines a standard port number for a key management connection, and the method further comprises the step of comparing in the received indicator packet a source port number against said standard port number for a key management connection.

18. A method for securely communicating packets between a first computer device and a second computer device through a packet-switched data transmission network comprising intermediate computer devices, where at least one of said computer devices performs a network address translation and/or a protocol conversion; where a security protocol is acknowledged which determines transport-mode processing of packets for

transmission and reception; and where a high-level protocol checksum has been determined for checking the integrity of received packets, the method comprising the steps of

- at the first computer device, performing transport-mode processing for packets to be transmitted to the second computer device,

- at the second computer device, performing transport-mode processing for packets received from the first computer device, said transport-mode processing comprising the decapsulation of received packets and

- at the second computer device, updating the high-level protocol checksum for decapsulated packets for compensating for changes, if any, caused by network address translations.

19. A method according to claim 18, wherein
- the step of performing transport-mode processing at the first computer device for packets transmitted to the second computer device takes the form of performing transport-mode processing as determined in the IPSEC protocol suite, and
- the step of performing transport-mode processing at the second computer device for packets received from the first computer device takes the form of performing transport-mode processing as determined in the IPSEC protocol suite.

20. A method according to claim 18, additionally comprising the steps of
- at the first computer device, after performing transport-mode processing for a packet to be transmitted to the second computer device, encapsulating the processed packet into a packet conforming to a certain second protocol, which second protocol is capable of traversing network address translations and
- at the second computer device, before performing transport-mode processing for a packet received from the first computer device, decapsulating the received packet from the packet conforming to said second protocol and replacing a number of network addresses in the decapsulated packet with a corresponding number of network addresses taken from the received packet before decapsulation.

21. A method according to claim 18, wherein the step of updating the high-level protocol checksum takes the form of recomputing the checksum for the transport-mode-processed packets.

22. A method according to claim 18, wherein the method additionally comprises the step of obtaining information about the network addresses of the first and second computer devices before and after network address translations, and the step of updating the high-level protocol checksum takes the form of incrementally updating the checksum based on the obtained information about the network addresses of the first and second computer devices before and after network address translations.

23. A method for maintaining the unchanged form of address translations performed by network address translation devices on encapsulated actual data packets transmitted with certain address information between a first computer device and a second computer device through a packet-switched data transmission network, the method comprising the step of

- forcing at least one of the first computer device and the second computer device to transmit to the other computer device keepalive packets with address information identical to that of actual data packets at a high enough frequency so that network

address translation devices constantly reuse the mappings used for network address translation even when a certain fraction of the packets communicated between the first computer device and the second computer device are lost in the network.

5

I hereby certify that this correspondence as being deposited with the United States Postal Service as express mail in an envelope addressed to: Commissioner of Patents and Trademarks. Washington D.C., 20231, on JUNE 15 19 99 Express Mail Receipt No. EM429087534US

JUNE 15, 1999 Ronald C. Fink

Date of Signature